Copy H.E.S.G
18/9.

15 (I)

TOP SECRET - 1 - TICOM/I - 100

Report by Uffz. HERZFELD of NAAST 5
(Gen. d. NA) on the work of the
Italian Referat of In.7/VI.

The attached report was written in English by HERZFELD at CSDIC(UK). See TICOM/I - 51,52, and SIR 1704 for earlier reports on HERZFELD.

TICOM No. of pages: 5

16th Sept. 1945.

Distribution.

British

D.D.3
D.D.4
D.D.(N.S.)
D.D.(M.W.)
D.D.(A.S.)
Lt. Col. Leathem
Cdr. Tandy
Major Morgan
Miss Mortimer (2)

U.S.

Op-20-G (2) (via Lt. Cdr. Manson)
G-2 (via Lt. Col. Hilles)
A.S.A. (3) (via Major Seaman)
Director, S.I.D. USFET
(via Lt. Col. Johnson)
Col. Lewis Powell, USSTAF

TICOM

Chairman
S.A.C. (2)
Cdr. Bacon
Lt. Col. Johnson
Major Seaman
Lt. Cdr. Manson
Capt. Cowan
Lt. Fehl
Ticom Files (2)

Unteroffizier HERZFELD
(HERZFELD's English)

WORK IN ITALIAN REFERAT

See TICOM/I - 51,52 and SIR 1704 for earlier reports on HERZFELD.

From July 1943 till the beginning of November 1943 PW worked in the Italian Referat of In/7/6. He was transferred there after ITALY had gone over to the Allies. A Führerbefehl had been issued stopping work on Italian ciphers in 1942. This work was now to be resumed. There was only a cadre Referat left when PW entered it. This consisted of Referatsleiter Uffz. MANAIGO and a small number of Unteroffiziere and Stabshelferinnen. PW was set to work on some 400 messages which had been intercepted in May, June and July. While this material was being statisticised by the Hollerith-Abteilung, PW worked on it at the Mathematiker-Referat together with Uffz. Dr. RINOW and Gefr. Regierungsrat WUNSCHE. The material consisted of 5Z (5 figure) messages of considerable length. In the course of August it was found out that the first and last group of each message was probably an indicator group. Very few repeats were found in the statistics obtained from Hollerith. In the beginning of September 1943 an Italian reciphering table and a number of messages from the cipher office of the Italian Commandantura at ATHENS arrived in BERLIN. They had been taken by some German officers under dramatic circumstances. When the news that MUSSOLINI had been arrested and that the Italian government had concluded an armistice, was received at German Headquarters in ATHENS, two lieutenants of Kommandeur der Nachrichtenaufklärung 4 at NEA PHALIRON drove to the commandantura in ODOS AMERIKIS in ATHENS, walked into the cipher office and started collecting the material lying on the tables in the office and packing it into a case in front of the bewildered cipher personnel. They were in the middle of doing so when a number of Italian officers came in and began shouting rather excitedly. After some controversy the Germans thought it preferable to disappear quietly since the attitude of the Italians became too threatening. They did however carry with them what they had collected from the tables and sent it on to BERLIN where PW was charged with trying to find out what it was worth.

The Reciphering table contained on its cover a note saying that it was to be used in connection with the code ELLADE and that the fact, that ELLADE code and reciphering had been used, was to be made clear by using certain 3-figure groups to indicate the use of this particular cipher. These 3-figure groups were given on the cover of the Reciphering block. There were about a dozen or a few more. Suppose they were:

076,095,122,187,234,335,545,577,678,777,829,867.

It was later found out from cipher material captured in Northern ITALY, that another code PIAVE and another reciphering table (or block) were in use in that district and that another set of some fifteen 3-figure groups like

008,029,255,267, a.s.o.

was used to indicate, that the cipher PIAVE was contained in that particular message.

1) Cipher Reference Group

PW soon found out that about 200 messages of a certain group of traffics in the BALKAN areas and the DODECANESE Islands always contained the 3-figure reference groups in the first, second and third figure of the first and of the last 5-figure group of each message. Thus one particular message may have begun with

67845..... .... and ended with..... .... 23478.

2) Reciphering Block With Indicator Groups

PW then inspected the reciphering table. It was in the form of a block, containing about 60 sheets. On some sheets figures had been written running from 8 to about 15. It was not difficult to guess that these were the date of the day on which that particular sheet of the table was to be used. The sheet was torn off the block and either destroyed or kept for some time for control purposes. Thus sheets bearing the written figures 1 to 7 had been torn off and were missing. Either the 7th or the 8th of August was therefore the date on which the German lieutenants had captured the block. Each page or sheet (as far as I remember one page of every sheet was printed) contained 1000 5-figure groups. On the top margin there were four lines of 2-figure groups, each line having ten such groups, so arranged as to have four different numbers to indicate each of the ten columns containing 100 of the 1000 5-figure groups. On the margin on the left there were four columns of 3-figure groups each column containing 100 numbers thus having four different numbers to indicate a certain line in the table. Thus every single 5-figure group out of the 1000 groups could be defined in the table by giving one of the four numbers on the top margin and one of the four numbers from the side margin indicating the line that contained the 5-figure group in question. The two numbers could be combined with each other to form a 5-figure group. This Indicator Group was "camouflaged" in the second and last but one group of the message.

3) Reciphering of Indicator Group.

PW soon found out that a small table containing 100 5-figure groups was used to recipher the indicator group. This assumption of PW was later confirmed when a TABELLINA was found to serve for "camouflaging" the indicator groups by adding to them a "camouflage group" (Tarngruppe), which was taken from this TABELLINA. The latter was to be used in connection with the PIAVE code discovered in Northern ITALY. The TABELLINA of the ELLADE code was not seized but PW was able to reconstruct it from the messages by assuming one Tarngruppe to be 00000. A 2-figure reference group was used to point out to the decipherer which Tarngruppe had been used. This "camouflage indicating group" (Tarnweiser) was combined with the cipher reference group to form the 5-figure group at the beginning and at the end of the message. Thus the groups given in the example under heading 1) are containing the Tarnweiser 45 and 78. The sums obtained by adding the respective Tarngruppen indicated by Tarnweiser 45 and 78 to the indicator group (for instance 78652) may be 83421 and 09608.

/These

These groups would then appear in the second and in the last but one group of the message, which would then begin and end with the following groups:

67845 83421 .... 09608 23478

When assuming that the Tarngruppe indicated by Tarnweiser 45 is 00000, and after subtracting this group from 83421 the latter is obviously the wanted indicator group. When this indicator group is subtracted from 09608, the Tarngruppe belonging to Tarnweiser 78 is obtained. It is

09608 - 83421 = 26287.

In this way PW constructed the TABELLINA of the ELADE code.

In the end of September 1943 PW obtained a fairly large amount of cipher material captured in Northern ITALY consisting of the PIAVE code, a reciphering table and a Tabellina as well as many messages. Work on this material was of course no crypto-analysis but simple decipherment. PW did however assume that since the PIAVE code was a 4-figure code having 20,000 positions (each 4-figure group having two meanings), the ELLADE code would be made up in the same way. Work on this code was interrupted when In 7/6 moved from BERLIN to JÜTERBOG in the middle of October 1943. PW resumed his work there, but in November 1943 Major LECHNER decided to dissolve the Italian Referat, a decision justified by the fact that after the fall of LEROS no more Italian wireless messages could be intercepted. It was believed that the Allies had prohibited further Italian wireless transmissions. PW was then transferred to the BALKAN Referat, the other members of the Referat to the French Referat and Uffz. MANAIGO, Uffz, KRATOCHVIL and Sdf. G BILDT were transferred to the Agenten Referat of Oberleutnant VAUCK.

Example of Sheet from a Reciphering Block.

				00	03	04	07	09	11	12	15	18	22
				49	47	46	45	41	37	33	29	28	26
				50	51	56	58	63	65	66	67	72	73
				98	96	94	93	91	88	85	83	79	76
001	498	500	997	46356	39806	65575	86487	45562	89556	42754	64806	65477	09768
003	497	504	995	20081	72915	09010	50829	24110	60513	26132	20601	18730	50316
005	495	506	993	06072	63384	51669	78274	49367	65478	27548	49026	18593	37561
	a.s.o.							a.s.o.					
248	254	743	751	21883	69450	89474	20011	12068	57427	96130	90302	94174	63756
249	252	749	750	63267	57291	88375	35901	43710	46382	44589	48928	76859	00153

1) Croatian State Ciphers

The Croat Army (Domobrani) and Ustaša were using a 5-figure code which was based on the former Yugoslav military code. Furthermore they used the German X-machine of the "Enigma" type. As far as PW knows there was no actual crypto-analytical work done in the Croat section of the BALKAN Referat but mostly deciphering and control work.

2) Hungarian Ciphers

PW believes that Wachtmeister Count ESZTERHAZY had been working successfully on a Hungarian code and a turning grille

(Drehraster) some time before PW entered the Balkan Referat. In the Autumn of 1944 PW remembers to have seen a number of Hungarian messages worked on by Uffz. TEUCHTLER and SEPER which he believes were enciphered by some sort of 2-figure substitution key of a somewhat more complicated type.

3) Rumanian Ciphers.

PW knows that Wachtmeister KARL SCHMIDT and Uffz. WAGNER have been working on a Rumanian diplomatic code consisting of 5-figure (or 6-figure?) groups.

4) Bulgarian Ciphers.

PW remembers that Uffz. THIELE worked on Bulgarian ciphers. PW has not seen his work and has therefore no knowledge of the type of cipher in question.

5) Turkish and Greek Ciphers.

All details known to PW have been mentioned in his report on his work at In 7/6 and on GREECE.